

Verifying Trust For Defense Use Commercial Semiconductors¹

Sydney Pope*, Brian S. Cohen, Vashisht Sharma**, Ryan R. Wagner**, Loren W. Linholm** and Sherry Gillespie*****

* OSD, Office of the Director, Industrial Policy

** Institute for Defense Analyses, Alexandria, VA

*** Potomac Institute for Policy Studies, Arlington, VA

Abstract: A systematic study identified verification techniques and assessed their effectiveness in identifying counterfeit and tampered integrated circuits from commercial sources acquired for DoD systems. Representatives of government, private industry, and academia helped identify and characterize key verification attributes and their overall effectiveness for each technique.

Keywords: Trust; Integrated Circuit; Trusted Defense Systems; Verification; Supply Chain; COTS; MOTS.

Introduction

The National Defense Authorization Act 110-417 for fiscal Year 2009, Section 254 requirement: Trusted Defense Systems directs the Department of Defense (DoD) to take action to address the need for a secure supply chain for semiconductor-based products essential to maintaining national security [1]. The supply chain for Integrated Circuits (ICs) is distributed across the globe and previous Institute for Defense Analyses (IDA) and external studies strongly suggest that these ICs are vulnerable to malicious tampering and counterfeiting. Section 254 (B) required that DoD to perform an assessment of methods that could be applied to verify the trust in commercial sources of ICs. This study was performed by the IDA assisted the DoD in responding to this request. IDA identified verification methods, collecting inputs from industry, academia, and government. These techniques were then evaluated in a workshop of DoD subject matter experts convened at IDA in July of 2009. The results of that evaluation formed the core of the results presented in this report.

The evaluation found a range of promising techniques and identified a number of low cost available techniques, mostly based on supplier pre-qualification and past performance assessments. Techniques for authentication and identifying ICs and their suppliers were found to be promising and are critical for enabling strong chain of custody security mechanisms. Simple incoming physical inspection techniques such as visual inspection and low cost testing were considered suitable for addressing counterfeit threats, although those techniques are unlikely to be effective against more detailed tampering and

malicious code. Where feasible, such as in the case of many commercially available ICs, hiding end-use can provide a degree of anonymity that inhibits an adversary's ability to target a defense system for insertion of adulterated components. Comparison techniques which performed physical analysis of products, primarily through imaging and reverse engineering were considered to be expensive and of diminishing effectiveness. These comparison techniques are unlikely to be broadly useful and will only be used for extremely critical components. The subject matter experts also identified a range of techniques such as reverse engineering, tools/techniques for design verification/validation, trusted anchor, advanced non-destructive soft X-ray techniques and others, requiring further research and development investments to address such threats and meet the needs of DoD.

Definitions and Methodology

Sec. 254 Trusted Defense Systems of the FY 09 NDAA (P.L. 110-417), requires an assessment of methods for verifying the trust of semiconductors procured from commercial sources. In response to this requirement, IDA undertook a systematic study to catalog verification techniques, and a methodology has been established to assess their effectiveness and applicability. Counterfeit and tampered ICs are becoming a major concern for the DoD as it relies more heavily on Commercial Off-The-Shelf (COTS) and Military Off-The-Shelf (MOTS) ICs. The intent of this assessment is to identify trust verification methods for ICs that can be implemented in the acquisition process in order to establish confidence that the ICs will not contain modified or tampered elements, will perform as expected, and that confidential information will not be exploited.

For the purposes of this study, verification was defined as "*the process of establishing confidence that the product will perform as expected and that confidential information has not been exploited.*"

In the evaluation of trust requirements for semiconductors, this study has defined three broad categories of criticality based on a simplification of the definitions used by the system assurance community [2]:

Criticality:

High - The compromise of the component results in direct, catastrophically degraded mission/business capability

¹ The publication of this paper does not indicate endorsement by the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of those organizations.

Moderate - The compromise of the component potentially results in partial or identifiable degradation to mission/business capability

Low - The compromise of the component potentially element potentially results in an inconvenience

The methodology employed for cataloguing verification techniques establish a taxonomy system to characterize techniques by type and application. A spreadsheet of key attributes was then distributed to approximately 65 stakeholders and technical experts in the DoD, the intelligence community, private industry, and academia. IDA requested them to complete the survey by filling in the spreadsheet for each technique.

Finally, the responders were asked to evaluate each technique they proposed, for cost, type of threat addressed, and state of maturity. The responders were asked to identify the pros and cons of each technique with regard to effectiveness and any positive or negative consequences of use. The types of threats being considered are counterfeiting, adversarial tampering, and loss of Intellectual Property (IP).

Based on the methods identified and information obtained in the survey, the workshop participants identified the most suitable methods for the DoD to employ. Feedback from the workshop participants on the state of maturity of the techniques allowed an assessment of the additional research and technology development needed for verification of trust of semiconductors that meet the needs of the DoD.

The strategy being developed to address ICs in trusted defense systems will promote the use of the verification tools/techniques identified for ensuring trust of commercially acquired components and systems. The policies and actions being developed promote the use and development of tools to verify trust in all phases of the IC development and production for mission-critical parts acquired from non-trusted sources. These phases include:

- Design
- Fabrication
- Distribution
- System integration
- Operations
- End of life

Identification of Verification Methods

A call for inputs was sent out to government, industry, and academia that resulted in a list of 65 verification methods. IDA normalized these verification methods by removing duplicates and combining methods that represented generalized or specialized versions of individual methods. IDA did not attempt to correct, refine, or rewrite the submitted verification methods except to combine as immediately apparent from the submitted text. This resulted in a list of 42 “suitable” methods as shown below:

Approved personnel	Auditing procedures and inventory control
Authentication and certification of vendors	Authorized/approved distributor
Classified applications engineering support	Control of scrap materials, out-of-specification devices, and/or suspect or confirmed defective, counterfeit, or tampered components
Control of surplus or overrun	Design tool source code and design data escrow
Design tool/library protection and validation	Deterrence of IC subversion via rapid attribution
Diminishing Manufacturing Sources and Material Shortages (DMSMS) management	Domestic ownership
EDA source code linting	Employing tools and techniques for design validation and protection
Failure analysis	Flow down
FPGA bitstream verification	GIDEP/ERAI
IC and photolithography validation to trusted design	Information Assurance best practices
Input fuzzing	Novel tamper detection techniques utilizing quantum or particle physics technology.
Physical inspections - external visual	Policy to protect IP and customer ID
Preferred vendors	Procurement anonymity
Quality Assurance best practices	Redundancy / N-version programming
Reverse engineering - mechanical delayering, layout comparison	Reverse engineering - advanced milling, imaging and comparison
RF interrogation of IC during operation	Standardization in design phase
Supplier financial/legal responsibility	Surrender counterfeits to dedicated repository
Testable Boundary	Testing and up screening
Tools and techniques for component verification and ID	Traceability/pedigree
Trusted anchor	Trusted foundry
Trusted supervision	Unique serial numbers to track ICs

Evaluation of Suitable Verification Methods

A workshop was held on July 16, 2009 at IDA to discuss the verification methods and to evaluate the suitability of each verification method. The workshop was attended by 42 US Government IC subject experts, knowledgeable in

areas such as research and development, test and evaluation, supply chain risk management analysis, procurement, and policy.

At the workshop, the participants were asked to discuss, review, and evaluate the verification methods with respect to categorization, cost, threat coverage, and maturity. Then the participants were asked to determine the suitability of the technique as one of the following:

Suitable for DoD:

- Only highly critical components
- Moderate and highly critical components
- Any components
- Never suitable
- No opinion

The results of the workshop were tabulated follow:

Suitable Techniques for Any Components: Available, broadly suitable techniques useful either at system engineering (component procurement) or during sustainment:

Low Cost

- Authentication and certification of vendors
- Authorized/approved distributor
- Flow down
- GIDEP/Electronics Retailers Association International (ERAI)
- Physical inspections - external visual
- Preferred vendors
- Quality Assurance best practices (such as ISO 9000 or QML)

Middle Cost

- Diminishing Manufacturing Sources and Material Shortages (DMSMS) management

Suitable Techniques for Moderately Critical ICs: Available, suitable techniques useful for moderately critical components either at system engineering (component procurement) or during sustainment:

Low Cost

- Auditing procedures and inventory control
- Control of scrap materials, out-of-specification devices, and/or suspect or confirmed defective, counterfeit, or tampered components
- Control of surplus or overruns
- Design tool/library protection and validation
- Information Assurance best practices
- Policy to protect IP and customer ID
- Supplier financial/legal responsibility

- Traceability/Pedigree

Middle Cost

- Approved personnel
- Failure analysis
- IC and photolithography validation to trusted design
- Procurement anonymity
- Testing and up screening
- Tools and techniques for component verification and ID
- Trusted foundry
- Unique serial numbers to track ICs

High Cost

- Domestic ownership

Suitable Techniques for Highly Critical ICs: Available, suitable techniques useful for highly critical components either at system engineering (component procurement) or during sustainment:

Low Cost

- Classified applications engineering support

Middle Cost

- FPGA bitstream verification
- Redundancy/N-version programming
- Standardization in design phase

High Cost

- Reverse engineering – mechanical delayering, layout comparison

Assessment for Counterfeiting and Tampering

Two major analyses were performed using the results of the catalogued verification methods and workshop feedback. First, IDA performed gap analysis focusing on identifying areas where verification methods could be applied by the DoD either at system engineering (when components were procured), or during operations/sustainment (when replacement supplies of components are procured). In the gap analysis, the overall suitability evaluation gauged the protection and the range of application provided by each of the verification methods. An assessment of coverage was developed both for the counterfeit threat and for all threats (counterfeiting, tampering, and IP theft). Next, an assessment of techniques that were identified as requiring further development or research were evaluated for suitability and cost.

This survey also identified a number of methods requiring further development or research. A comprehensive description of this study and an analysis and summary of the results can be found elsewhere [3].

Analysis - Protecting Against Counterfeiting

The analysis suggests that there are serious gaps at design and at end-of-life (EOL) and weak protection at operations (OPS) during sustainment.

Available low cost solutions that protect design and EOL;

- Authentication/Certification of vendors/preferred vendors

Available low cost solutions that protect OPS:

- GIDEP/ERAI
- Authentication/Certification of vendors/preferred vendors
- Quality Assurance

Analysis - Protecting Against Tampering

The analysis found that there is generally weak protection across the life cycle and serious gaps at design and EOL.

Serious gaps at Design and EOL:

- Weak protection at system engineering
- Physical inspections – external visual
- Preferred vendors

Summary

This study examined a broad range of proposed verification techniques. The specific proposals in many instances require additional refinement in order to be considered as appropriate to recommend for DOD action. The study of verification techniques found several low cost, readily available methods for managing most IC supply chain threats. The majority of these are supplier pre-qualification and past-performance assessment programs (such as supplier/distributor authorization, authentication, certification, pre-approval, and quality best practices). These can be widely employed to meet DoD requirements and are a primary method used by industry for promoting product assurance, especially from a quality, safety, and security perspective. Adaptation of these programs can also mitigate, but will not eliminate the risk of counterfeit or tampered ICs from insertion into defense systems as shown by recent Department of Justice indictments.

Where feasible, such as for many commercially available ICs, hiding end-use can provide a degree of anonymity that inhibits an adversary's ability to target a defense system for the insertion of adulterated components. However, the use of this method limits communication with the supplier base

and may inhibit the early detection of component performance and life-cycle sustainment problems. In addition, end-use anonymity may not be successful if the ICs are unique to intended defense systems applications through function, performance, or system environment. End-use anonymity was assessed to be potential high value; however, additional research is required.

Among the more promising techniques suggested by many workshop participants were those for identifying and authenticating ICs and subsequent tracking by using unique serial identification numbers. These techniques would enable a much greater resistance to unauthorized ICs entering the defense supply chain and provide a fundamental control mechanism to enable detailed chain of custody and chain of evidence.

Comparison techniques, where ICs are compared against one of known pedigree, and destructive physical analysis are considered to be prohibitively expensive and of diminishing effectiveness. Comprehensive electrical testing commensurate with the criticality of end-use is being practiced as a quality control, but is a cost-prohibitive means for assuring the quality of most ICs. It can also degrade product reliability and service life. Attempts to use these techniques to detect intentional defects (introduced by counterfeiting or tampering) makes their application impractical when the detection rate is below the rate of unintentional manufacturing defects.

Physical inspections and low cost testing techniques are suitable for addressing most counterfeit threats. They are, however, less effective against sophisticated forms of counterfeiting and not effective for detecting circuits containing malicious code.

References

1. NDAA 2009, Section 254 Trusted Defense Systems, Public Law 110-417, (http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ110.110.pdf).
2. Engineering For System Assurance, Version 1.0, NDIA, October 2008, (<http://www.acq.osd.mil/sse/docs/SA-Guidebook-v1-Oct2008.pdf>).
3. Cohen, B. S., Sharma, V., Wagner, R., Linholm, L., Gillespie, S., Holzer, J., "Assessment of Methods for Verifying the Trust of Semiconductors Procured from Commercial Sources," IDA Document D-3937, to be published.